2-Factor Authentication Introduction

To help prevent someone stealing your password through phishing or scamming, Regis utilizes a **2-Factor Authentication** process, which adds an extra layer of security to your account.

When **2-Factor Authentication** is in place, a user logging into Microsoft 365 is required to prove they have both the password and access to something ONLY the user should have, such as a personal phone.

With **2-Factor Authentication**, if a Regis employee or student falls for a phishing scam and provides their password to a scammer, the scammer won't be able to log into Microsoft 365 without having access to that personal device/phone. The employee/student will know that another person is trying to log into their account when they receive authorization notification that they didn't request.

NOTE: If you receive a two-factor code that you did not request, **CHANGE YOUR PASSWORD IMMEDIATELY** and contact the ITS Helpdesk as quickly as possible in person or by the phone at **781-768-7177**.

Multifactor Authentication

Microsoft introduced a new process for authenticating who is trying to log in. With this process, called Multifactor Authentication (MFA) push notification using Authenticator, you will be presented with a number. Type that number into the Authenticator app to complete the approval.

Why is MS Authenticator asking for a Number?
Microsoft's Authenticator app's number matching feature requires users to type the number displayed on the sign-in screen to approve access requests. It helps to counter Multi-Factor Authentication (MFA) fatigue attacks that rely on push notification spam.

Number matching is a key security upgrade to traditional second factor notifications in Microsoft Authenticator.